MEMORANDUM OF AGREEMENT

BETWEEN

THE DEPARTMENT OF HOMELAND SECURITY

AND

City of Houston, Texas

I. PURPOSE. This Memorandum of Agreement (MOA) describes the partnership and responsibilities of the Department of Homeland Security (DHS), acting through the Office of Intelligence and Analysis (I&A) and the City of Houston, each individually, "Party," and collectively, "Parties," in an effort to:

(1) Provide direct national level intelligence support to the Host through the assignment of DHS personnel to serve as an interface between the Host and the national Intelligence Community (IC) (as defined in 50 U.S.C. 401a) in order to facilitate intelligence and information sharing consistent with the law;

(2) Manage, analyze, fuse, tailor and disseminate information in accordance with applicable laws, rules, regulations and authorities, and to facilitate the identification and prevention of threats within the scope of DHS's authority, as defined generally by the Homeland Security Act of 2002, as amended, and Executive Order 12333, as amended;

(3) Provide DHS support and coordination to the principal officials of the designated Host fusion center, Federal, State, local, tribal, and private sector homeland security officials, and the officer designated as the Homeland Security Advisor of that State, in accordance with section V of this MOA, 6 U.S.C. § 124h, and in addition to those specific functions assigned elsewhere in law to DHS/I&A;

(4) Improve communication and coordination among Federal, State, local, tribal and private sector organizations and assist in developing methods to exchange relevant information in support of homeland security responsibilities of each organization.

II. AUTHORITY. This MOA is entered into by DHS pursuant to the Homeland Security Act of 2002, as amended, 6 U.S.C. §§ 121(d), 124h, 481, and 482; the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. §485; Executive Order 13311, "Homeland Security Information Sharing," July 29, 2003; Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," Oct. 25, 2005; and Executive Order 12333, "United States Intelligence Activities," Dec. 4, 1981, as amended.

The City of Houston is a municipal corporation and home-rule City able to enter into this agreement pursuant to its corporate and general powers as enumerated under the City of Houston Charter Article II Section 1 and 2.

III. DEFINITIONS. For purposes of this MOA, the following terms shall have the following meanings when used herein:

A. "Classified Information" has the meaning given that term in 50 U.S.C. § 426, that is, information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

B. "Sensitive But Unclassified Information" shall refer generally to unclassified information in the possession of either Party to this MOA to which access controls or distribution limitations have been applied in accordance with applicable laws, policies, or regulations. It may include any locally-defined handling caveat or marking authorized for use by either party. It also includes unclassified information in the possession of the U.S. Government that may be exempt from public disclosure or subject to other controls.

C. "Fusion center" means a collaborative effort of two or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal, terrorist, or other activity related to homeland security.

D. "DHS Officer" shall mean any DHS employee who is to perform intelligence analysis, reporting, or liaison functions and act as an official DHS representative to the designated Host fusion center. This individual will not perform duties as an employee or official representative of the Host.

E. "Homeland Security Information" has the meaning given that term in 6 U.S.C. § 482, that is, any information possessed by a Federal, State, or local agency that (a) relates to the threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act. Such information may be "Classified Information" or "Sensitive but Unclassified Information."

F. "Joint-seal intelligence product" means a finished intelligence product in any format which is represented as the combined work product of both the Host and DHS. In some instances, such products may feature the seals or letterhead identifying both the Host and DHS.

G. "Information sharing environment" means the information sharing environment established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. §485.

H. "Intelligence analyst" means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military conditions, trends, or forces in foreign or domestic areas that

directly or indirectly affect national or homeland security.

I. "Intelligence-led policing" means the collection and analysis of information to produce an intelligence product designed to inform law enforcement decision making at the tactical and strategic levels.

J. "Terrorism information" has the meaning given that term in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485, that is, all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—(a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individual to the United States, United States persons, or United States interests, or to those of other nations; (c) communications of or by such groups or individuals; or (d) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and includes weapons of mass destruction information.

K. "Personally Identifiable Information" (PII) means information which can be used to distinguish or trace an the identity of a U.S. Citizen or lawful permanent resident, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

L. "Privacy Incident" means the suspected or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII in usable form, whether physical or electronic.

IV. SCOPE.

A. Nothing in this MOA shall be construed as encroaching upon the sovereign rights, privileges, and immunities of either Party, by the other, in the conduct of inherently Municipal, State or Federal government operations, except as may be authorized pursuant to the U.S. Constitution. Nothing in this MOA is intended to conflict with current law, regulation, or the policies and directives of DHS or the Host. If a term or condition of this MOA is inconsistent with such authorities, the Parties agree to address and resolve the inconsistency in a timely and legally appropriate manner, unless the matter is incapable of timely resolution, in which case the inconsistent term shall be deemed invalid, but the remaining terms and conditions of this MOA shall remain in full-force and effect.

B. This MOA, in and of itself, does not result in the commitment, obligation, or transfer of funds or other financial obligations between the Parties. No provision of this MOA shall be interpreted to require obligation or payment of funds in violation of the Anti-Deficiency Act,

Title 31 U.S.C. § 1341.

C. The following activities are specifically excluded from this MOA:

(1) Short-term (usually no more than 30 days) operational DHS support, including through temporary assignments of DHS personnel, to the Host.

(2) Assignments or Intergovernmental Details, per other formal agreements, which are based on cooperative joint training efforts in which training population drives instructor and support assignments for the training.

(3) Assignment of contractor personnel to the Host to perform contractor services in support of DHS.

V. RESPONSIBILITIES.

A. **DHS Responsibilities.** DHS shall select and assign, on a non-reimbursable basis, one or more DHS Officers to coordinate with and facilitate DHS support to the Host in the exchange of relevant intelligence and information consistent with applicable federal statutes, executive orders, Department regulations and policies. DHS will:

(1) establish a rotational assignment policy that contemplates both the optimum level of support to the Host and the professional development of the individual employee assigned as a DHS Officer;

(2) ensure that the assigned DHS Officer is provided secure data and telecommunications systems capabilities in appropriately certified and secured space and facilities provided by the Host;

(3) provide appropriate training to Host personnel, and perform other activities as authorized in support of the administration of DHS' training program, to include: intelligence analysis or information sharing training incorporating an intelligence-led policing curriculum that is consistent with standard training and education programs offered to DHS law enforcement and intelligence personnel; privacy and civil liberties training that is developed, supported, or sponsored by the DHS Chief Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties; and such other training as prescribed by the Under Secretary for I&A;

(4) ensure, to the extent practicable, any anticipated or expected absence of a DHS Officer which exceeds 30 consecutive days is covered by the temporary assignment of a DHS Officer in a manner consistent with ensuring continuous support to the Host;

(5) provide necessary personnel management/human capital support for DHS Officers, in accordance with Office of Personnel Management (hereinafter "OPM") and DHS regulations and guidelines, including consideration for promotions, awards, and other administrative actions.

B. **Host Responsibilities.** The Host shall, consistent with applicable Federal and State

statutes, regulations, executive orders and policies:

(1) provide office space, parking, unclassified data and telecommunications systems, and any administrative office supplies necessary to perform the tasks under this MOA;

(2) provide access to all Host facilities, equipment, and technical information as may be required to perform the duties outlined in this MOA;

(3) consistent with applicable authorities, policies and procedures of the Parties, provide access to Host databases, reports, investigations, and other information produced, retained, and/or controlled by the Host in order to review this information and assist the Host in identifying the types of information, including enforcement information, that may assist DHS or other entities with homeland security responsibilities;

(4) as appropriate, issue and/or disseminate DHS and joint seal intelligence products consistent with dissemination guidance provided by DHS or in coordination with and following the concurrence of the DHS Officer assigned to the Host; and

(5) promptly notify DHS following a privacy incident involving information originating with DHS.

C. **DHS Officer Responsibilities.** Consistent with their functional duties and responsibilities as designated by DHS, DHS Officers will:

(1) provide analytic and reporting advice; training, and assistance;

(2) coordinate with the Host to identify information needs and transform them into information requirements and product requests;

(3) track information requests and the delivery of responsive information and intelligence products and provide feedback from the Host to the producers;

(4) create intelligence and other information products derived from such information and other homeland security-relevant information provided by DHS;

(5) consistent with applicable authority and in accordance with the principles outlined in Section VI of this agreement, access relevant databases, reports, investigations, and other information produced, retained, and/or controlled by the Host in order to review this information and assist the Host in identifying the types of law enforcement information and information that may assist DHS or other entities protecting the United States;

(6) support efforts of the Host to report information that may assist DHS fulfill its mission, as well as support other entities protecting the United States;

(7) support efforts of the Host to participate in the information sharing environment;

(8) coordinate with other relevant Federal entities engaged in homeland security-related activities;

(9) carry out such other duties as the Secretary of Homeland Security determines are appropriate;

(10) refrain from exercising any supervisory or disciplinary authority over personnel of the Host's facility or participating offices; and

(11) ensure that products intended to be issued and/or disseminated by the Host as joint-seal intelligence products have been reviewed and cleared by DHS according to established DHS procedures for disseminating finished intelligence products.

(12) be familiar with the policy and procedures of the Houston Regional Intelligence Service Center.

VI. INFORMATION SHARING AND HANDLING

A. **Key Principles.** The following key principles and standards apply to the sharing of information between the Parties in any form including verbal, paper, electronic, audio and visual:

(1) sharing must always be in furtherance of the official duties undertaken by the Parties;

(2) the originator of the information to be shared is considered to be the owner of that information and is accountable for deciding how information will be shared in a manner that will ensure the timely and efficient access by the Parties to all information necessary to discharge their official duties;

(3) the Parties will ensure that information will be appropriately marked to indicate the presence of handling, safeguarding, or dissemination controls and is provided with the expectation that these controls will be preserved;

(4) the sharing of PII must be limited to that which is reasonably necessary for the intended recipient to understand, assess, or act on the information provided;

(5) privacy policies and relevant privacy compliance documents, such as Privacy Act notices (including systems of records notices and "(e)(3)" or similar notices) will be issued, reviewed, and revised as appropriate to ensure that they properly describe the treatment of PII;

(6) information sharing must comply with all applicable laws, regulations, or procedures and will incorporate protection mechanisms for handling of proprietary information;

(7) the use of data by an employee of either Party in an unauthorized or illegal manner will result in a review of the factual circumstances by both Parties and potentially subject the employee to appropriate remedial actions;

(8) to maintain data accuracy, where necessary, the Parties will be informed of any changes to the data they have received and also notify the source of any error they discover;

(9) the Parties will ensure that all staff are educated to manage sensitive information appropriately consistent with these principles and organizational policy on the collection and uses of information during the performance of official duties;

(10) the Parties will ensure that any third parties providing a service to them agree and abide by these principles by inclusion in contracts/agreements;

(11) dissemination of information from one Party to another shall not be considered a release of information to the public, nor shall it constitute a waiver of any exemption to the release of information under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 or similar state law;

(12) any Party in receipt of a request for information (whether pursuant to a FOIA, "sunshine," or discovery law) whose scope includes information shared by the other Party or documents developed jointly by the Parties, shall (a) consult with that Party prior to any disclosure, with the aim of developing a consensus view regarding an appropriate response, or (b) refer the request to the originating Party for a direct response to the requester; and

(13) information will be classified, marked, and accessed, as appropriate, pursuant to Executive Order 12958, as amended and Executive Order 12968; and

(14) joint-seal intelligence products will be issued and/or disseminated in accordance with both parties' policies and clearance procedures.

B. Notwithstanding the paragraphs above, the Parties may use, disclose, reproduce, or retain, in accordance with the law of the State and applicable Host policy, any Party-provided data or information (except data or information properly classified in accordance with Executive Order 12958) that is or was:

(1) already in the public domain at the time or which thereafter enters the public domain without fault or breach of this MOA by the Party;

(2) already made known to or lawfully acquired from a third party by the Party;

(3) previously disclosed to the Party without restriction from the other Party; or

(4) provided or disclosed to, or independently acquired by, the Party without restrictions from its originating source.

C. Notwithstanding the paragraphs above, pursuant to 6 U.S.C. § 482, information obtained by a State or local government from a Federal agency shall remain under the control of the Federal agency, and a State or local law authorizing or requiring such a government to disclose information shall not apply to such information. The State or local agency shall: (a) withhold such information from any response; (b) release such information only with the expressed approval of the Federal agency; or (c) refer the request to the originating Federal agency for a direct response to the requester.

VII. SECURITY REQUIREMENTS.

A. The DHS Officers, in order to meet his or her mission objectives, shall have appropriate access to all relevant Federal databases and information systems, consistent with any applicable policies, guidelines, procedures, instructions, or standards established by the President or, the program manager of the Information sharing environment for the implementation and management of that environment, or as otherwise limited by federal law. This shall require that at a minimum, the DHS Officers must have an active security clearance at the level of Top Secret, and be read-on to SCI accesses as required.

B. Host will provide the DHS Officer with any local clearance or access necessary to accomplish duties consistent with DHS's mission responsibilities.

C. Host will protect the identity and personal information of the DHS Officer from public disclosure and will refer all inquiries regarding the presence of the DHS Officer to the DHS Public Affairs Office.

D. For purposes of access to Host information, the DHS Officer shall be considered a federal law enforcement, intelligence, protective, national defense, immigration, or national security official, and shall be considered by Host as authorized to receive information from law enforcement agencies.

VIII. DISCIPLINE AND REMOVAL.

A. Federal employees are subject to the Ethics in Government Act of 1978, 5 C.F.R. part 735, which regulates employee responsibilities and conduct; the Federal Trade Secrets Act, 18 USC, Section 1905; as well as DHS-specific standards of conduct regulations;

B. The Host may not take disciplinary or other administrative action against a DHS Officer who commits a violation under similar Host procedures and regulations governing the conduct of Host employees. DHS however, will take such administrative or disciplinary action against the DHS Officer as may be appropriate under the specific circumstance;

C. The assignment of a DHS Officer can be terminated or modified at any time at the option of DHS or the Host for any reason, including, but not limited to, the DHS Officer's violation of the laws, regulations, or policies of the Host. Where possible, the Party desiring to terminate or modify the assignment should provide a 90-day notice to the other Party. This

notification should be in writing and should include the reasons for the termination or modification. A DHS Officer must be removed immediately from his assignment whenever that DHS Officer ceases to be employed by DHS. DHS will select, assess and train a suitable replacement for any DHS Officer removed under this Section, consistent with the requirements of this MOA.

IX. DISPUTES.

A. Disputes arising under or relating to this MOA shall be resolved only through consultations between the Parties. The dispute shall not be referred to any outside Party or to any other forum for settlement without the consent of both Parties.

B. The Host will not pursue any claims against the U.S. Government or its employees, including, but not limited to claims for money, reimbursement of expenses, benefits or salaries paid to any of the Host's employees for its compliance with the responsibilities described within the terms of this MOA. This provision not to pursue any claims applies to past, present, and future compliance with the responsibilities described within the terms of this MOA and is retroactive to and includes claims for compliance with the responsibilities previously provided by the Host to DHS that are consistent with the responsibilities described within the terms of this MOA. This MOA does not waive remedies otherwise available to the Host under the Federal Tort Claims Act or other federal legislation expressly authorizing a private right of action for damages against the U.S. Government.

X. OTHER PROVISIONS.

A. Nothing in this MOA is intended to conflict with current law or regulation or the directives of either Party. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

B. Under the Inspector General Act of 1978, as amended, 5 USC App. 3, a review of this MOA may be conducted at any time. The Inspector General of the Department of Homeland Security, or any of his or her duly authorized representatives, shall have access to materials of the Parties, consistent with applicable authorities of the Parties, in order to perform audits, inspections, investigations, or other examinations of the DHS officers, as authorized by law.

C. Any travel or training will be processed through travel orders with applicable reimbursement paid by the Party that requested and authorized the travel or training. All DHS Officer travel and training will be conducted in accordance with applicable DHS Management Directives and regulations, and the Federal Travel Regulations.

D. Nothing in this MOA shall, or is intended to confer any substantive or procedural right, and this MOA shall not be construed to create a private right of action for enforcement of any of its provisions or a defense to noncompliance with any independently applicable legal obligation.

XI. ENTRY INTO FORCE, AMENDMENT, DURATION AND TERMINATION.

A. All obligations of the Parties under this MOA shall be subject to the availability of properly authorized and appropriated funds for such purposes.

B. This MOA shall become effective upon signature by both Parties and shall remain in effect for an indefinite period.

C. This MOA may be amended by the written agreement of both Parties.

D. This MOA shall supersede any and all prior arrangements regarding DHS Officers entered into by the Parties or their respective organizations, units, or agencies.

E. This MOA may be terminated at will by any party upon ninety (90) days after written notification to the other Party.

F. This MOA may be signed in counterparts, each of which shall be considered to be an original.

For the Department of Homeland Security:

Deputy Under Secretary for Intelligence & Analysis
Department of Homeland Security

Date: 3/31/11

For the City of Houston

Mayor's Office of Public Safety &
Homeland Security

Date: 2-11-11

MEMORANDUM OF AGREEMENT

BETWEEN

THE DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INTELLIGENCE AND ANALYSIS (I&A)

AND

HOUSTON POLICE DEPARTMENT

I. PARTIES. This Memorandum of Agreement (hereinafter "MOA"), entered into between the Department of Homeland Security (hereinafter "DHS"), through the Office of Intelligence and Analysis (hereinafter "I&A"), and the Houston Police Department, (hereinafter "Host"), each individually, "Party", and collectively, "Parties", provides for the detailing of personnel from DHS to the Host.

II. AUTHORITY. This MOA is entered into by DHS pursuant to 6 USC §§ 121(d) and 124h, sections 201(d) and 210A of the Homeland Security Act of 2002, as amended, the Intelligence Reform and Terrorism Prevention Act (hereinafter "IRTPA") of 2004, Executive Order (hereinafter "E.O.") 13311 of July 29, 2003, Homeland Security Information Sharing, E.O. 13356 of August 27, 2004, Strengthening the Sharing of Terrorism Information To Protect Americans, and E.O. 13388 of October 25, 2005, Further Strengthening the Sharing of Terrorism Information To Protect Americans.

III. DEFINITIONS. In addition to any terms defined in other provisions of this MOA, the following terms shall have the following meanings when used herein:

A. "Classified Information" shall mean official U.S. Government information that requires protection in the interests of national security and is so designated by the application of security classification markings and protections outlined in Executive Order 12958, as amended, entitled "Classified National Security Information;"

B. "SBU, LES and ORCON Information" shall refer to unclassified information in the possession of either Party to this MOA to which access or distribution limitations have been applied in accordance with applicable laws, policies, or regulations. Sensitive But Unclassified (hereinafter "SBU"), Law Enforcement Sensitive (hereinafter "LES"), Originator Controlled (hereinafter "ORCON"), and any other locally-defined handling caveats fall into this category. It also includes information in the possession of the U. S. Government that is exempt from public disclosure or subject to other controls;

C. "Senior Intelligence Officer" shall mean the DHS person who is to perform duties as the Senior Intelligence Officer (hereinafter "DHS SIO") and act as an official representative of I&A and DHS. This individual will not perform duties as an official representative of the Host;

D. "Fusion center" means a collaborative effort of 2 or more Federal, State, local, or tribal government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend,

and respond to criminal or terrorist activity;

E. "Information sharing environment" means the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

F. "Intelligence analyst" means an individual who regularly advises, administers, supervises, or performs work in the collection, gathering, analysis, evaluation, reporting, production, or dissemination of information on political, economic, social, cultural, physical, geographical, scientific, or military conditions, trends, or forces in foreign or domestic areas that directly or indirectly affect national security;

G. "Intelligence-led policing" means the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision making at the tactical and strategic levels; and

H. "Terrorism information" has the meaning given that term in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

IV. SCOPE.

A Nothing in this MOA shall be construed as Federal encroachment into State or local government operations. Nothing in this MOA is intended to conflict with current law, or regulation, or the directives of DHS or the Host. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full-force and effect.

B. This MOA, in and of itself, does not result in transfer of funds or other financial obligations between the Parties. No provision of this MOA shall be interpreted to require obligation or payment of funds in violation of the Anti-Deficiency Act, Title 31 U.S.C. § 1341.

C. The following details or assignments are specifically excluded from this MOA:

(1) Short-term (usually no more than 30 days) operational DHS support to the Host.

(2) Details per other formal agreements which are based on cooperative joint training efforts in which training population drives instructor and support assignments for the training.

(3) Assignment of contractor personnel to the Host to perform contractor services in support of DHS.

D. The DHS SIO may serve as a liaison to only one major agency of the Host at any time.

V. PURPOSE.

A. The establishment of the DHS SIO position under this MOA shall be based upon the Host's meeting of the qualifying criteria for a fusion center, their acceptance of the DHS SIO, and the demonstrated and continuing need for, and the mutual benefit of, this position to both Parties. Once established, the DHS SIO position shall be subject to periodic review by both Parties to validate a continuing need for the position. Where a valid need for the position no longer exists, or if the qualifying criteria are no longer met,

the Parties agree that the position shall be subject to elimination. Performance under this MOA by both Parties is subject to the availability of personnel and funding.

B. This MOA describes the partnership and responsibilities of the Parties in an effort to:

- Provide direct national level intelligence support to the State through the assignment of DHS personnel to serve as a primary interface between the State and the national Intelligence Community (IC) in order to fulfill intelligence and information sharing consistent with the law;
- Manage, analyze, fuse, tailor and disseminate information, to include law enforcement information collected from Federal, State, local, tribal, and private sector sources, to facilitate the identification and prevention of threats within the scope of DHS's authority, as defined by the Homeland Security Act of 2002, as amended;
- As appropriate, in addition to the functions in 6 USC 121(d), section 201(d) of the Homeland Security Act of 2002, as amended, assist in the performance of the functions below:

  (1) provide operational and intelligence advice and assistance to State, local, and regional fusion centers;

  (2) support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment;

  (3) conduct tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, and regional fusion centers to integrate the efforts of such networks with the efforts of the Department;

  (4) coordinate with other relevant Federal entities engaged in homeland security-related activities;

  (5) provide analytic and reporting advice and assistance to State, local, and regional fusion centers;

  (6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and to incorporate such information, as appropriate, into the Department's own such information;

  (7) provide management assistance to State, local, and regional fusion centers;

  (8) serve as a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information;

  (9) facilitate close communication and coordination between State, local, and regional fusion centers and the Department;

  (10) provide State, local, and regional fusion centers with expertise on Department resources and operations;

  (11) provide training to State, local, and regional fusion centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department; and

  (12) carry out such other duties as the Secretary determines are appropriate.

The functions in subsection V.B. of this MOA above may only be carried out with the express approval of I&A. Routine tasks of the DHS SIO are addressed in section VI.C. below.

VI. RESPONSIBILITIES.
DHS shall be responsible for:

A. Selecting and assigning, on a non-reimbursable basis, a DHS SIO to support the Host in the exchange of relevant intelligence and information consistent with the law. Barring other circumstances, DHS will establish a rotation and assignment policy that contemplates both the optimum level of support to the Host and the professional development of the individual employee assigned as a DHS SIO;

B. Ensuring that any DHS SIO shall be considered for familiarity with the State, locality, or region, as determined by such factors as whether the DHS SIO has been previously assigned in the geographic area; or has previously worked with intelligence officials or law enforcement or other emergency response providers from that State, locality, or region. Before being assigned to a fusion center, the DHS SIO shall undergo:
(i) appropriate intelligence analysis or information sharing training using an intelligence-led policing curriculum that is consistent with--
(I) standard training and education programs offered to Department law enforcement and intelligence personnel; and
(II) the Criminal Intelligence Systems Operating Policies under part 23 of title 28, Code of Federal Regulations (or any corresponding similar rule or regulation);
(ii) appropriate privacy and civil liberties training that is developed, supported, or sponsored by the Privacy Officer appointed under section 222 [6 USCS § 142] and the Officer for Civil Rights and Civil Liberties of the Department, in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004 (5 U.S.C. 601 note);
(iii) Intelligence oversight / US Person information handling procedures training; and
(iv) such other training prescribed by the Under Secretary for I&A.

C. Representing DHS mission requirements to the Host and developing and maintaining an information sharing relationship between the Host and DHS consistent with the Homeland Security Act of 2002, as amended. To accomplish this, the DHS SIO's primary duties are outlined in subsections (1) through (7) below. Additionally, with the express authorization of I&A, the DHS SIO may perform some or all of the functions in section V.B. of this MOA. The DHS SIO will:

(1) assist law enforcement agencies and other emergency response providers of State, local, and tribal governments and fusion center personnel in using information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, to develop a comprehensive and accurate threat picture;

(2) review homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;

(3) create intelligence and other information products derived from such information and other homeland security-relevant information provided by DHS;

(4) assist in the dissemination of such products, as coordinated by the Under Secretary for I&A, to law enforcement agencies and other emergency response providers of State, local, and tribal government, other fusion centers, and appropriate Federal agencies;

(5) Coordinate with the Host to identify Host's information needs and transform them into information requirements and product requests;

(6) Track information requests and the delivery of final products undertaken by DHS, evaluate final products for Host information requirement satisfaction, and provide feedback from the Host to the producers; and

(7) Have access to all databases, reports, investigations, and other information produced, retained, and/or controlled by the Host in order to review this information and assist the Host in identifying the types of law enforcement information and information resident at the Host that may assist DHS and the broad spectrum of federal and non-federal entities engaged in protecting the United States homeland. The DHS SIO will help facilitate the communication of that information to DHS.

D. Ensuring that appropriate measures are taken, consistent with Federal law, rules and regulations, to notify DHS employees that all protected information received from the Host is:

(1) Protected from unauthorized disclosure;

(2) To be used only in the performance of official duties;

(3) To be classified, as appropriate, pursuant to Executive Order 12958, as amended, and other applicable federal classification directives; and

(4) To be shared, retained, and disseminated in a manner consistent with the guidance and procedures mandated by the Director of National Intelligence to protect intelligence sources and methods and similar guidance of the Attorney General concerning the handling of sensitive law enforcement information.

Notwithstanding the above, DHS shall not be restricted in use, disclosure, and reproduction of any data that falls into the following categories: data in the public domain at the time of disclosure or which thereafter enters the public domain without breach of this MOA; data known to DHS at the time of disclosure; data that has been disclosed to DHS without restriction from the Host; and data that has become known to DHS without similar restrictions from a source

F. Refraining from exercising any supervisory or disciplinary authority over personnel of the Host's facility or office.

G. Requiring the DHS SIO to provide biweekly significant activity summaries to DHS.

H. Ensuring that the assigned DHS SIO is provided secure communications and data systems capabilities throughout the duration of this MOA in spaces and facilities otherwise provided by the Host.

I. Providing training to Host personnel as required or necessary, and performing other activities in support of the administration of DHS' training program.

J. Traveling as necessary to support the Host. This includes local travel to attend conferences and meetings as required. The Host is not authorized to task the DHS SIO to travel outside the local area (25 miles from primary work location) without advance coordination with DHS. Travel outside of the local area on official business will require the processing of travel requests through DHS. The DHS SIO is required to provide an after-action report (hereinafter "AAR") for any conference or meeting the DHS SIO attends in the course of performing the duties outlined in this MOA, and that is paid for by DHS. .

K. To the extent possible, ensuring that any anticipated or expected absence of a DHS SIO which exceeds 14 consecutive days is backstopped by DHS in a manner consistent with ensuring continuous support to the Host; and

L. Providing for the DHS SIO, all necessary administrative and logistical support in accordance with Office of Personnel Management (hereinafter "OPM") and Departmental regulations and guidelines, including consideration for promotions, awards, and other administrative actions.

The Host shall be responsible for:

A. Providing office space, parking, an unclassified computer system and telephone, and any administrative office supplies necessary to perform the tasks under this MOA;

B. Providing access to all its facilities, equipment, and technical information as may be required to perform the duties outlined in this MOA;

C. Providing access to the DHS SIO to all databases, reports, investigations, and other information produced, retained, and/or controlled by the Host in order to review this information and assist the Host in identifying the types of law enforcement information and classified information resident at the Host that may assist DHS and the broad spectrum of federal and non-federal entities engaged in protecting the United States homeland; and

D. Ensuring that, as a condition of receipt of data or information provided by DHS to the Host pursuant to activities covered by this MOA, procedures are instituted to ensure that such information shall, under its law, be deemed to remain under the full and exclusive control of the Federal government for the purpose of determining its authorized release to the public. Moreover, these procedures shall ensure that the release of such information to the Host shall not be considered a release of information "to the public" and shall not constitute a waiver by DHS of any applicable exemption to the release of such information required under the Freedom of Information Act (5 U.S.C. § 552). These procedures shall reflect that the exclusive means for releasing such information to the public is either at the sole discretion of DHS, or pursuant to a formal request submitted under the Freedom of Information Act (5 U.S.C. § 552). Unless otherwise stated, sensitive Information provided by DHS to the Host, and appropriately marked to indicate the presence of handling or dissemination controls, is provided with a clear expectation that the confidentiality of this sensitive information will be preserved. DHS provided information shall be accepted by the Host pursuant to these safeguards and assurances only.

Notwithstanding the above, the Host shall not be restricted in use, disclosure, and reproduction of any data or information that falls into the following categories: data in the public domain at the time of disclosure or which thereafter enters the public domain without breach of this MOA; data known to the Host at the time of disclosure; data that has been disclosed to the Host without restriction from DHS; and data that has become known to the Host without similar restrictions from a source.

VII. SECURITY REQUIREMENTS.

A. The DHS SIO, in order to meet his or her mission objectives, shall have appropriate access to all relevant Federal databases and information systems, consistent with any policies, guidelines, procedures, instructions, or standards established by the President or, as appropriate, the program manager of the information sharing environment for the implementation and management of that environment. This shall include at a minimum, an active security clearance at the level of Top Secret, and read on to SCI access, including SI, G, TK, and HCS.

B. Host will read-on the DHS SIO for any local clearance access necessary to accomplish duties consistent with DHS's mission and I&A's responsibilities.

VIII. DISCIPLINE AND REMOVAL.

A. Federal employees are subject to the Ethics in Government Act of 1978, 5 C.F.R. part 735, which regulates employee responsibilities and conduct; as well as DHS-specific standards of conduct regulations.

B. The Host may not take disciplinary or other administrative action against a DHS SIO who commits a violation under similar Host procedures and regulations governing the conduct of Host employees. DHS however, will take such administrative or disciplinary action against the DHS SIO as may be appropriate under those

circumstances. The Parties shall cooperate in the investigation of any violations of the laws or regulations of either Party.

C. The assignment of a DHS SIO can be withdrawn, modified or curtailed at any time at the option of DHS or the Host for any reason, including, but not limited to, the DHS SIO's violation of the laws, regulations, or policies of the Host. Where possible, the Party desiring to terminate the MOA prior to the expiration of this MOA should give a 90-day notice to the other Party. This notification should be in writing and should include the reasons for the termination. Any DHS SIO must be removed immediately from his assignment whenever that DHS SIO ceases to be employed by DHS. DHS will select, assess and train a suitable replacement for any DHS SIO removed under this Section, provided the replacement meets the requirements of this MOA.

IX. DISPUTES.

A. Disputes arising under or relating to this MOA shall be resolved only through consultations between the Parties. The dispute shall not be referred to any outside Party or to any other forum for settlement without the consent of both Parties.

B. The Host will not pursue any claims against the U.S. Government or its employees, including, but not limited to claims for money, reimbursement of expenses, benefits or salaries paid to any of the Host's employees for its compliance with the responsibilities described within the terms of this MOA. This provision not to pursue any claims applies to past, present, and future compliance with the responsibilities described within the terms of this MOA and is retroactive to and includes claims for compliance with the responsibilities previously provided by the Host to DHS that are consistent with the responsibilities described within the terms of this MOA. This MOA does not waive remedies otherwise available to the Host under the Federal Tort Claims Act or other federal legislation expressly authorizing a private right of action for damages against the U.S. Government.

X. OTHER PROVISIONS.

A. Nothing in this MOA is intended to conflict with current law or regulation or the directives of either Party. If a term of this MOA is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

B. Under the Inspector General Act of 1978, as amended, 5 USC App. 3, a review of this MOA may be conducted at any time. The Inspector General of the Department of Homeland Security, or any of his or her duly authorized representatives, shall have access to any pertinent books, documents, papers and records of the Parties to this MOA, whether written, printed, recorded, produced, or reproduced by any mechanical, magnetic or other process or medium, in order to make audits, inspections, excerpts, transcripts, or other examinations as authorized by law.

C. Any travel or training will be processed through travel orders with applicable reimbursement paid by the Party that requested and authorized the travel or training.

D. Nothing in this MOA shall, or is intended to confer any substantive or procedural right, and this MOA shall not be construed to create a private right of action for enforcement of any of its provisions or a defense to noncompliance with any independently applicable legal obligation.

XI. ENTRY INTO FORCE, AMENDMENT, DURATION AND TERMINATION.

A. All obligations of the Parties under this MOA shall be subject to State and Federal laws, as appropriate and the availability of properly authorized and appropriated funds for such purposes.

B. DHS shall instruct the DHS SIO on all obligations and restrictions applicable to him or her under this MOA.

C. This MOA may be amended by the mutual written agreement of the Parties, and changes to this MOA shall be formalized by a written amendment by both Parties that shall describe the nature of the change. Changes to this MOA shall be signed at the same level as the signatories to this MOA. Either Party may terminate this MOA upon ninety (90) days after written notification to the other Party.

D. Upon the earlier of, the completion of the DHS SIO's detail, or the expiration or termination of this MOA, each Party shall make arrangements to remove the DHS SIO from the Host.

E. This MOA shall supersede any and all prior arrangements regarding the DHS SIO position entered into by the Parties or their respective organizations, units, or agencies.

F. This MOA shall become effective upon signature by both Parties. This MOA shall remain in effect for two years, unless sooner terminated or modified, and may be extended by written mutual agreement of the Parties.

For the Department of Homeland Security:

Chief Intelligence Officer
Department of Homeland Security

Date: 20 Nov 08

Houston Police Department

Chief of Police

Date: 10-6-08

507

Houston Regional Intelligence Service Center (HRISC)
Memorandum of Understanding

This Memorandum of Understanding (MOU) is entered into by the Houston Police Department and the below listed agencies, and outlines participation in the Houston Regional Intelligence Service Center (HRISC). The listed agencies hereafter referred to as "participant agencies," jointly and severally agree to abide by the terms and provisions of this MOU throughout its duration. In order to ensure aggressive capability to prevent, detect, respond and recover from a terrorist act, the Houston/Harris County region has established a regional intelligence service.

The Harris County Sheriffs Department (HCSO)
The Texas Department of Public Safety (DPS)
The Metropolitan Transit Authority Police (METRO)
Federal Bureau of Investigation (Houston Office)

Purpose:

The purpose of this Memorandum of Understanding is to set out a common understanding and agreement of the policies and procedures that participant agencies will follow in providing a regional counter-terrorist and criminal intelligence service in the furtherance of protecting the lives and property of the citizenry. This Memorandum of Understanding is not intended to be legally binding on any of the signing parties of this document.

Mission:

The mission of the Houston Regional Intelligence Service Center (referred hereafter also as the "Center") is to provide continuous security to our region by gathering, developing and sharing intelligence into the capabilities, intentions, and actions of terrorist groups and individuals which pose a threat to our populace and region.

Organization - Chain of Command

- **Personnel**

  Personnel assigned to the captioned Center will consist of a combined body of members who are assigned or attached to, or are in active association with, the Houston Regional Intelligence Service Center.

  Members shall be considered as full time participants in the Center if they spend at least sixty percent of their effort towards the Center's mission and are physically collocated at the Center. Members shall be considered as Associates if they contribute to the mission of the Center and are virtually or electronically collocated with the Center.

- **Direction of the Houston Regional Intelligence Service Center**

  All participants, acting as equal partners, acknowledge the mission of the Houston Regional Intelligence Service Center, and will work in concert towards fulfillment of the mission. The policy, program involvement, and direction of the service shall be the responsibility of the Chief of Police of the Houston Police Department or his designee who will coordinate with the designated members of the participating agencies.

- **Operational Oversight & Supervision**

  General supervision of the personnel assigned to the Houston Regional Intelligence Service Center will be the responsibility of the participating agencies. Day to day supervision and operational oversight, however, of the intelligence service and its direction, shall be with a Houston Police Department supervisor who will act as the administrative coordinator of the center.

  The responsibility for the conduct of individuals assigned to the center remains with their respective agency.

- **Operational Personnel**

  The Houston Police Department initially agrees to assign four (4) officers to the Center, as well as provide positions for one or more officers/agents from the participating agencies. Full participating agencies will provide, at a minimum, one officer or agent or member full time to the service center. The Houston Police Department will also provide positions for a minimum of two analysts within the Center. Associate participants will designate a contact person within their agency to liaison and interact with the Center.

- **Office Space, Equipment, Vehicles, Overtime**

  The Houston Police Department agrees to provide office space, equipment and supplies, to carry out the administrative operation of the Houston Regional Intelligence Service Center. Additional equipment required by an agency will be the responsibility of that agency.

  Vehicles and overtime will be the responsibility of each individual agency pursuant to their policies.

Procedures

- **Compliance with Regulations**

  The Houston Regional Intelligence Service Center, and the personnel assigned there, will operate in compliance with federal regulations regarding intelligence, specifically 28 CFR Part 23 et al.

  The Houston Regional Intelligence Service Center shall develop procedural guidelines to ensure operational and informational security as well as to provide for the effective and efficient operation of the Center.

- **Assignment of Personnel**

  Personnel assigned to the Center will be assigned matters and duties related to the mission of the Intelligence Center. Continued assignment of members will be based upon performance, and will be at the discretion of the respective participating agencies in coordination with HPD.

- **Information Exchange & Intelligence Sharing**

  Participating agencies agree to exchange and share information to the Center in furtherance of its mission; connectivity back to the participant agency's information, database, data warehouse is required.

  In order to ensure the rights of innocent citizens are not abridged, all intelligence products and intelligence sharing shall adhere to the rules in keeping with 28 CFR Part 23 et al and the "need to know/right to know" standard. To prevent compromise of intelligence products produced, access and dissemination will be controlled and all intelligence products produced will be labeled "Law Enforcement Sensitive, For Official Use Only."

Amendments to this MOU

If the signatory parties agree, this MOU may be amended at any time in the future to include additional participating agencies.

Duration

There is no limit as to the term of this Memorandum of Understanding. However, any party wishing to terminate participation may do so by providing written notice to the other parties of their intent to withdraw from this agreement.

By: _____ Date: 7-5-07

Harold H. Hurtt, Chief of Police
Houston Police Department

By: Roderick L. Beverly Date: 5/2/07

Roderick Beverly, Special Agent in Charge
Federal Bureau of Investigation (Houston Office)

Houston Regional Intelligence Service Center (HRISC)
Memorandum of Understanding

This Memorandum of Understanding (MOU) is entered into by the Houston Police Department and the below listed agencies, and outlines participation in the Houston Regional Intelligence Service Center (HRISC). The listed agencies hereafter referred to as "participant agencies," jointly and severally agree to abide by the terms and provisions of this MOU throughout its duration. In order to ensure aggressive capability to prevent, detect, respond and recover from a terrorist act, the Houston/Harris County region has established a regional intelligence service.

The Harris County Sheriffs Department (HCSO)
The Texas Department of Public Safety (DPS)
The Metropolitan Transit Authority Police (METRO)

Purpose:

The purpose of this Memorandum of Understanding is to set out a common understanding and agreement of the policies and procedures that participant agencies will follow in providing a regional counter-terrorist and criminal intelligence service in the furtherance of protecting the lives and property of the citizenry. This Memorandum of Understanding is not intended to be legally binding on any of the signing parties of this document.

Mission:

The mission of the Houston Regional Intelligence Service Center (referred hereafter also as the "Center") is to provide continuous security to our region by gathering, developing and sharing intelligence into the capabilities, intentions, and actions of terrorist groups and individuals which pose a threat to our populace and region.

Organization - Chain of Command

- **Personnel**

  Personnel assigned to the captioned Center will consist of a combined body of members who are assigned or attached to, or are in active association with, the Houston Regional Intelligence Service Center.

  Members shall be considered as full time participants in the Center if they spend at least sixty percent of their effort towards the Center's mission and are physically collocated at the Center. Members shall be considered as Associates if they contribute to the mission of the Center and are virtually or electronically collocated with the Center.

- **Direction of the Houston Regional Intelligence Service Center**

  All participants, acting as equal partners, acknowledge the mission of the Houston Regional Intelligence Service Center, and will work in concert towards fulfillment of the mission. The policy, program involvement, and direction of the service shall be the responsibility of the Chief of Police of the Houston Police Department or his designee who will coordinate with the designated members of the participating agencies.

- **Operational Oversight & Supervision**

  General supervision of the personnel assigned to the Houston Regional Intelligence Service Center will be the responsibility of the participating agencies. Day to day supervision and operational oversight, however, of the intelligence service and its direction, shall be with a Houston Police Department supervisor who will act as the administrative coordinator of the center.

  The responsibility for the conduct of individuals assigned to the center remains with their respective agency.

- **Operational Personnel**

  The Houston Police Department initially agrees to assign four (4) officers to the Center, as well as provide positions for one or more officers/agents from the participating agencies. Full participating agencies will provide, at a minimum, one officer or agent or member full time to the service center. The Houston Police Department will also provide positions for a minimum of two analysts within the Center. Associate participants will designate a contact person within their agency to liaison and interact with the Center.

- **Office Space, Equipment, Vehicles, Overtime**

  The Houston Police Department agrees to provide office space, equipment and supplies, to carry out the administrative operation of the Houston Regional Intelligence Service Center. Additional equipment required by an agency will be the responsibility of that agency.

  Vehicles and overtime will be the responsibility of each individual agency pursuant to their policies.

Procedures

- **Compliance with Regulations**

  The Houston Regional Intelligence Service Center, and the personnel assigned there, will operate in compliance with federal regulations regarding intelligence, specifically 28 CFR Part 23 et al.

  The Houston Regional Intelligence Service Center shall develop procedural guidelines to ensure operational and informational security as well as to provide for the effective and efficient operation of the Center.

- **Assignment of Personnel**

  Personnel assigned to the Center will be assigned matters and duties related to the mission of the Intelligence Center. Continued assignment of members will be based upon performance, and will be at the discretion of the respective participating agencies in coordination with HPD.

- **Information Exchange & Intelligence Sharing**

  Participating agencies agree to exchange and share information to the Center in furtherance of its mission; connectivity back to the participant agency's information, database, data warehouse is required.

  In order to ensure the rights of innocent citizens are not abridged, all intelligence products and intelligence sharing shall adhere to the rules in keeping with 28 CFR Part 23 et al and the "need to know/right to know" standard. To prevent compromise of intelligence products produced, access and dissemination will be controlled and all intelligence products produced will be labeled "Law Enforcement Sensitive, For Official Use Only."

Amendments to this MOU

If the signatory parties agree, this MOU may be amended at any time in the future to include additional participating agencies.

Duration

There is no limit as to the term of this Memorandum of Understanding. However, any party wishing to terminate participation may do so by providing written notice to the other parties of their intent to withdraw from this agreement.

11-15-06

By: C. A. McClelland, Acting Chief of Police Date: _____

Harold L. Hurtt, Chief of Police
Houston Police Department

By: _____ Date: 12-15-06

Tommy Thomas, Sheriff
Harris County Sheriff's Office

By: _____ Date: 2/06/2007

Honorable Robert Eckels
Harris County Judge

By: Thomas A. Davis Jr. Date: 2-9-07

Thomas A. Davis Jr., Director
Texas Department of Public Safety

By: _____ Date: 12-20-06

Thomas C. Lambert, Chief
Metropolitan Transit Authority Police Department

F35-682
I406-101

CITY OF HOUSTON

INTER OFFICE CORRESPONDENCE

TO: T. N. Oettmeier, Executive Assistant Chief
Patrol Operations

VIA: D. S. Perales, Assistant Chief
Special Investigations Command

M. W. Thaler, Executive Assistant Chief
Investigative Operations

FROM: R. W. Holland, Captain
Criminal Intelligence Division

DATE: May 14, 2007

SUBJECT: **Addition to the Memorandum of Understanding for the Houston Regional Intelligence Service Center**

The Federal Bureau of Investigation (FBI) has offered to place an FBI analyst at the Houston Regional Intelligence Service Center (HRISC), and they are currently working on acquiring equipment and developing building requirements that will allow their analyst to have access to their secure databases.

Currently, there is an MOU that was signed by the original members of the HRISC that I modified by adding the FBI to the signature page. Attached is that MOU that was signed by Special Agent in Charge Roderick Beverly and a copy of the original HRISC MOU.

Should you have any questions please contact me.

R. W. Holland, Captain
Criminal Intelligence Division

rwh:rm
Attachments

acting SAC

RECEIVED
07 MAY 21 PM 2:08
ASSISTANT CHIEF
M.W. THALER

CITY OF HOUSTON

INTER OFFICE CORRESPONDENCE

TO: Harold L. Hurtt
Chief of Police

FROM: T. N. Oettmeier, Executive Assistant Chief
Patrol Operations

DATE: June 28, 2007

SUBJECT: **Memorandum of Understanding: Houston Regional Intelligence Service Center**

The attached Memorandum of Understanding for the Houston Regional Intelligence Service Center and HPD is provided for your review and signature.

There is already an active MOU that excludes the Federal Bureau of Investigation. The attached MOU adds a signature line for the FBI to be included. I am attaching the original MOU for your reference, as well as the new MOU for your signature and review.

Our Legal Services Unit has reviewed and approved this MOU. I agree that it is beneficial for our department to enter this MOU.

Your signature is needed on the original attached. An original will be kept on file in the Patrol Operations office and an copy will be sent to the Federal Bureau of Investigation.

T. N. Oettmeier, Executive Assistant Chief
Patrol Operations

tno:rkp

Attachment

OFFICE OF THE CHIEF OF POLICE
2007 JUL -2 PM 12:19

DESIGNATED STATE FUSION CENTER

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

HOUSTON POLICE DEPARTMENT
(Houston Regional Intelligence Service Center)
(Fusion Center)

PREAMBLE

The timely sharing of intelligence between federal, state, local, tribal and private sector partners is a central and critical component in preventing or mitigating threats. State fusion centers (SFCs) and multi-agency intelligence centers (MAICs) are important focal points for federal, state, and local information and intelligence sharing. The establishment of SFCs and MAICs to combine the intelligence and information sharing efforts of all participating agencies will enhance our ability to predict, prevent, and respond to unlawful activity and threats to our nation.

This Memorandum of Understanding (MOU) is entered into between the Houston Police Department (Houston Regional Intelligence Service Center) and the Federal Bureau of Investigation (FBI) hereinafter referred to as "the Parties".

I. PURPOSE

A. The purpose of this MOU is to set forth the terms by which the FBI agrees to commit personnel resources and to contribute information to the Houston Regional Intelligence Service Center. This effort will continue to improve communication and coordination among federal, state, local, tribal, and private sector organizations and assist in developing methods to combine relevant information at all levels to maximize the usefulness of all available information.

B. By entering into this MOU, the Parties agree to and incorporate by reference the Fusion Center Charter (*or similar fusion center operating documents*) , which sets forth the Mission, Goals, Functions, Management Principles, Membership, Staffing, Policies/Protocols (including privacy policy), and other provisions relating to the establishment, organization, and operation of the Houston Regional Intelligence Service Center.

C. This MOU is an agreement among the Parties and is not intended, and should not be construed, to create or confer on any other person or entity any right or benefit, substantive or procedural, enforceable at law or otherwise against the FBI, the Department of Justice, the United States, the Fusion Center, or any State, locality, or other sponsor under whose auspices a party is participating in the Fusion Center, or the officers, directors, employees, detailees, agents, representatives, task force members, contractors, subcontractors, consultants, advisors, successors, assignees or other agencies thereof.

II. MISSION

The SFC/MAIC environment complements the FBI's existing field capability to provide an optimum environment for advancing mission objectives and goals across all FBI programs. A full partnership with the SFC/MAIC represents a key element of optimizing our combined reach and extending our capacity through robust interaction with state, local, tribal and private sector partners. The FBI's involvement in the SFC/MAIC further enhances the ability to provide those tools which assist law enforcement in intelligence-led policing. This partnership will further develop the requirements management process which translates the needs of intelligence customers into requirements to collect information, produce intelligence reports, and disseminate intelligence to those who need it.

Field Intelligence Groups (FIGs) are and will remain the focal point for FBI intelligence activity in the field. Through integration or the assignment of personnel they extend that role into the specialized needs of Joint Terrorism Task Forces (JTTFs) and fusion centers. Each has a distinct, but interdependent function; FIGs managing and providing oversight to the effective application of intelligence in support of FBI's mission; the intelligence components of JTTFs focused on enabling the detection, pursuit and disruption of terrorist threats; and Fusion Centers as a focal point for extending and interweaving a network of information exchange and partnership to achieve a true capacity for domain management.

The Houston Regional Intelligence Service Center (fusion center) was organized in response to the attacks of September 11th, 2001, and the other continuing threats to the greater Houston region and its community. While some may believe that the fusion center concept is a new one it has actually evolved from a decade long cooperative spirit born out of multi-agency task forces and cross-discipline relationships in response to crime. From these relationships and shared experiences, our departments and agencies have developed a collegiality which makes fusion centers a functional reality.

Mission Statement

The mission of the Houston Regional Intelligence Service Center (fusion center) is to provide continuous security to our region by gathering, developing and sharing intelligence into the capabilities, intentions, and actions of terrorist groups and individuals which pose a threat to our populace and region.

III. AUTHORITY

Pursuant to 28 U.S.C. ' 533, 28 C.F.R. ' 0.85, Executive Order 12333, and Annex II to National Security Presidential Decision Directive (NSPD) 46/Homeland Security Presidential Directive (HSPD) 15, the FBI is authorized to coordinate an intelligence, investigative, and operational response to terrorism and other major crimes within both state and federal jurisdictions. By virtue of that same authority, the FBI is participating in the Houston Regional Intelligence Service Center that is composed of other federal, state, local, tribal and private sector organizations acting in support of the above listed statutory and regulatory provisions.

The full time participating agencies are the Houston Police Department, the Harris County Sheriff's Office, the Texas Department of Public Safety, and the Houston Metropolitan Police Department. Other nearby counties, incorporated jurisdictions and school and university police departments participate as virtual partners providing incident reporting and intelligence sharing.

IV. CONTROLLING DOCUMENTS

A. Since the FBI operates under the authority of the Attorney General of the United States, all FBI participants must adhere to applicable Attorney General's Guidelines and directives, to include the following-as amended or supplemented:

1. Attorney General's Guidelines for Domestic FBI Operations (September 29, 2008);

2. Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations (May 30, 2002);

3. Attorney General Memorandum dated March 6, 2002, titled Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI;

4. Attorney General's Guidelines for Confidential Human Sources (effective June 13, 2007);

5. Memorandum from the Deputy Attorney General and the FBI Director regarding: Field Guidance on Intelligence Sharing Procedures for [Foreign Intelligence] and [Foreign Counterintelligence] Investigations (December 24, 2002); and

6. Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (March 4, 2003).

B. All guidance on investigative matters handled by the FBI will be issued by the Attorney General and the FBI, to include the FBI "Domestic Investigations and Operations Guide" of December 16, 2008 (or successor editions). The FBI will provide copies of the above-listed guidelines and any other applicable policies for reference and review to all cleared Fusion Center members to the extent such documents do not contain sensitive or privileged information. This MOU does not alter or abrogate existing directives or policies regarding the conduct of investigations or the use of special investigative techniques or confidential human sources.

V. STAFFING COMMITMENT

A. As a Fusion Center Member Agency, the FBI hereby agrees to be a Principal Member of the Fusion Center, as described in the Charter and, based on available staffing, shall contribute the following resources to the Fusion Center:

The FBI agrees to assign one (1) Intelligence Analyst, to the Houston Regional Intelligence Service Center. Absent extraordinary circumstances, any FBI Agent or Intelligence Analyst designated by the FBI to be detailed to the Houston Regional Intelligence Service Center, will be detailed for a minimum period of one (1) year. Personnel detailed by the FBI to the Fusion Center shall bold and maintain a Top Secret/SCI clearance or bold and maintain a minimum of a Secret clearance, with a request for Top Secret/SCI clearance in process.

B. Responsibility for the conduct of each FBI Fusion Center assignee, both personally and professionally, shall remain with the FBI. During this detail, FBI employees will continue to work under the rules and regulations applicable to the FBI's employees and will be subject to the same personnel rules, regulations, laws and policies, including ethical standards, applicable to those employees. FBI employees will comply with FBI rules pertaining to outside employment and prepublication review requirements and will remain subject to the Supplemental Standards of Ethical Conduct for Employees of the Department of Justice. FBI assignees will report personnel and administrative matters to the FBI designated Fusion Center representative.

VI. RECORDS, REPORTS AND INFORMATION SHARING

A. Information in FBI information systems will be disseminated to Fusion Center partners in accordance with federal statutes and regulations, court orders, Executive Orders, Department of Justice and FBI guidelines and policies, and information sharing policy and provisions of the FBI Intelligence Policy Manual. FBI information extracted from investigative and intelligence files, or any FBI information system, and disseminated to Fusion Center partners, may not be: 1. further disseminated outside the Fusion Center; 2. entered into a Fusion Center generated report intended for external dissemination; or 3.used as a basis for investigative or law enforcement activity by Fusion Center partners without the approval of the FBI Fusion Center representative. If the dissemination of FBI information results in a request or demand for that (or related) information from FBI files under federal law, or state law including state "sunshine" or freedom of information laws, or federal or state criminal discovery, the request or demand will be referred to the FBI field office and processed under regulations issued by the Attorney General in 28 Code of Federal Regulations, Part 16.

B. To the extent information received as a result of this MOU is the subject of or is responsive to a request for information under the Freedom of Information Act, the Privacy Act, or a Congressional inquiry, such disclosure may only be made after consultation with and only upon approval of the FBI.

C. Terrorism related threat information will continue to flow to the Joint Terrorism Task Force (JTTF) as the recognized and designated environment in which Federal-to-local operational partnerships take place to detect, investigate, and disrupt terrorist threats or pursue perpetrators.

D. Terrorist Screening Center (TSC). In addition to the other provisions of Section VI, the sharing of terrorist screening information from the TSC has additional restrictions. All parties to this MOU acknowledge that it is the policy of the U.S. Government to neither confirm nor deny watchlist status. Information about whether a person is on a terrorist watchlist is proprietary information of the TSC and is a federal record provided to fusion centers under this MOU only for intelligence and lead purposes. In order to protect the operational interests of the FBI and other government agencies who contribute information to TSC, information obtained from the TSC will not be used in affidavits, subpoenas, or submissions in legal, judicial, or administrative proceedings, unless expressly authorized in writing by the Director of the TSC. Any violation of this subsection may be grounds for withholding future access to TSC terrorist screening

information by the offending individuals and/or Parties, or may be grounds for terminating this MOU.

VII. FUNDING

This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of the understanding between the Parties to commit resources to the Fusion Center. Unless otherwise agreed in writing, each Party shall bear its own costs in relation to this MOU. Expenditures by each Party will be subject to each organization's budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that the above language in no way implies that Congress will appropriate additional funds for such expenditures.

VIII. MEDIA

Media releases relating to FBI intelligence or operational activity will be mutually agreed upon and jointly handled by the member Participating Agencies of the Fusion Center.

IX. PRIVACY AND CIVIL LIBERTIES

A. The Parties agree to comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information through the Fusion Center, including, to the extent applicable, the privacy guidelines established for the Information Sharing Environment created by §1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.

B. Each Party agrees to review and make appropriate changes, if any, to their privacy compliance documents, including, with respect to federal parties, applicable Privacy Act system of records notices, (e)(3) notices, and privacy policies (including policies applicable to the Information Sharing Environment) in advance of the implementation of this MOU to ensure that the scope and routine uses of such notices and policies permit the collection, maintenance and sharing of personal information as set forth in this MOU and, with respect to non-federal parties, applicable requirements imposed by state privacy laws.

C. Each party agrees that the Fusion Center has now, or will develop, a privacy policy that comports, to the extent practicable, with the Privacy

Policy Development Guide published by the Department of Justice as part of the Global Information Sharing Initiative.

D. This MOU does not alter the Parties' civil and financial liabilities, if any and pursuant to applicable law. The FBI shall not be responsible for any civil or financial claim which does not arise from an act or omission of an employee of the FBI.

E. Information provided to state or local government partners by the FBI under this MOU will remain under the control of the FBI and shall be exempt from state or local government law authorizing or requiring the disclosure of such information, including homeland security information in accordance with Section 892(e) of the Homeland Security Act of 2002.

X. DURATION

A. The term of the MOU continues in force until terminated. The MOU may be terminated at will by any party, as long as written notice is provided to the other parties of not less than sixty (60) days. Upon termination of the MOU, all equipment will be returned to the supplying party.

B. Notwithstanding this provision, the provisions of Paragraph VI, entitled RECORDS, REPORTS AND INFORMATION SHARING will continue until all potential liabilities have survived termination of this MOU.

XI. SECURITY FOR FBI INFORMATION AND INFORMATION SYSTEMS

The following requirements will be complied with where classified FBI documents are stored at or used at the fusion center, or where classified FBI information systems and removable media, including but not limited to FBINet and subsystems accessed through FBINet, are installed and accessible at the fusion center.

A. No classified documents, classified removable media, or classified information systems will be permitted into the fusion center space until the space where the classified materials are to be housed has been inspected and approved by the DHS Office of Security, Administrative Security Division, Policy Implementation & Oversight Branch or the FBI Security Division, Security Operations Section, Physical Security Unit as complying with requirements for storage of classified materials, and

certified as to the conditions for use of the space and storage of classified material as either open or closed storage.

B. All communications security equipment will be handled only by FBI personnel, regardless of the clearance level granted to other fusion center personnel. FBI personnel will be responsible for removal and storage of all communications security equipment, to include coders, taclanes, and removable hard drives or other media.

C. At no time shall FBINet or other classified FBI information systems be connected to any other information system. Any problems with or maintenance required by FBINet or other classified FBI information systems shall be addressed by FBI Information Technology Specialists.

D. All fusion center personnel who will have access to space in which classified FBI documents, removable media, or information systems will be present shall obtain **at minimum a** "Secret" level clearance and attend a briefing by the FBI Chief Security Officer regarding the proper use, handling, dissemination, and destruction of classified FBI documents, removable media, and information systems. At that time the personnel will also execute an SF-312 and/or FD-868 non-disclosure form, and upon ceasing participation in the fusion center or surrendering their clearance will be debriefed on their continuing obligations regarding disclosure of classified information and execute an SF-312 debrief form.

E. Any actual, suspected, or possible improper disclosure of classified material or compromise of classified information systems will be immediately reported to the cognizant Security Officer for the fusion center and the FBI personnel detailed to the fusion center. The FBI personnel detailed to the fusion center shall, upon notification of the incident, report to their FBI Chief Security Officer.

X. AMENDMENTS

This MOU in no manner affects any existing MOUs or agreements with the FBI or any other agency. This MOU may be amended only by mutual written consent of the parties. The modifications shall have no force and effect unless such modifications are reduced to writing and signed by an authorized representative of the FBI and the Fusion Center.

SIGNATORIES:

_____ Date: _____

(Assistant Director in Charge/Special Agent in Charge)

_____ Date: 6-11-11

Charles A. McClelland, Jr.
Chief of Police